

Michiel Kusters - Universiteit Leiden
mkusters@math.leidenuniv.nl, October 3, 2011

Anisotropy and the integral closure

1. ABSTRACT

Let K be a number field and let A be an order in K . The trace map from K to \mathbf{Q} induces a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle : B \times B \rightarrow \mathbf{Q}/\mathbf{Z}$ where B is a certain finite abelian group of size $\Delta(A)$. In this article we discuss how one can obtain information about \mathcal{O}_K by purely looking at this symmetric bilinear form. The concepts of *anisotropy* and *quasi-anisotropy*, as defined in another article by the author, turn out to be very useful. We will for example show that under certain assumptions one can obtain \mathcal{O}_K directly from $\langle \cdot, \cdot \rangle$.

In this article we will work in a more general setting than we have discussed above. We consider orders over Dedekind domains.

2. INTRODUCTION

We will discuss the relation between the new concepts of anisotropy and quasi-anisotropy as defined in [6] and the integral closure of an order in its total quotient ring. These concepts show that in some cases one can find explicit formulas for the integral closure.

All rings in this article are assumed to be commutative.

We will first discuss some practical versions of the theorems which we will prove in this article. First let B be a finite abelian group, with additive notation. Then we define the *lower root* of B as

$$\text{lr}(B) = \sum_{r \in \mathbf{Z}} rB \cap B[r],$$

where $B[r] = \{b \in B : rb = 0\}$. Let α be an algebraic integer and let $K = \mathbf{Q}(\alpha)$ and $A = \mathbf{Z}[\alpha]$. One has a trace map $\text{Tr}_{K/\mathbf{Q}} : K \rightarrow \mathbf{Q}$. Now define the *trace dual* of A as

$$A^\dagger = \{x \in K : \text{Tr}(xA) \subseteq \mathbf{Z}\}.$$

It turns out that A^\dagger contains A and that A^\dagger/A is a finite abelian group. Let $\overline{A} = \mathcal{O}_K$ be the integral closure of A in K . Our goal is to determine \overline{A} .

The starting point of the theory which we develop in this article, is the following theorem (see Section 10).

Theorem 2.1. *Let $p \in \mathbf{Z}$ be prime and assume that $p > [K : \mathbf{Q}]$. Then we have $p \mid \exp(\overline{A}/A)$ if and only if $p^2 \mid \exp(A^\dagger/A)$, where \exp stands for the exponent of the corresponding group.*

Using this theorem one can prove that, under the assumption that a certain form is anisotropic or quasi-anisotropic, \mathcal{O}_K corresponds to the lower root of A^\dagger/A . For example, one has following theorem, which uses the concept of anisotropy (see Section 10).

Theorem 2.2. Suppose that $B = A^\dagger/A$ and that $2 \nmid \#B$. Suppose that $B \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m'\mathbf{Z}$, where $m = \prod_p \text{prime } p^{n(p)}$ and similarly $m' = \prod_p \text{prime } p^{n'(p)}$ such that for all primes p we have $n(p)n'(p) = 0$ or $n(p) + n'(p)$ is odd. Then $\overline{A}/A = \text{lr}(A^\dagger/A)$.

Using quasi-anisotropy (and some other techniques) one finds a stronger version. In order to find the integral closure, it is enough to find the integral closure locally. We have the following theorem (see Section 15).

Theorem 2.3. Let $\mathfrak{m} \subset A$ be a maximal ideal, let $p\mathbf{Z} = \mathfrak{m} \cap \mathbf{Z}$. Define the numbers $n(i)$ such that $(A^\dagger/A)_\mathfrak{m} \cong \bigoplus_{i \geq 1} (\mathbf{Z}/p^i\mathbf{Z})^{n(i)}$. Suppose that the following conditions are satisfied.

- i. $p > \sum_{i \geq 1} n(i)$;
- ii. There exist $i_1, i_2 \in \mathbf{Z}_{\geq 1}$ such that
 - $i_1 \not\equiv i_2 \pmod{2}$;
 - $n(i) = 0$ for all $i \notin \{1, i_1, i_2\}$;
 - $n(i) \in \{0, [A/\mathfrak{m} : \mathbf{Z}/p\mathbf{Z}]\}$ for $i \in \{i_1, i_2\}$.

Then one has $(\overline{A}/A)_\mathfrak{m} = \text{lr}((A^\dagger/A)_\mathfrak{m})$.

In this article we will prove the results above in a more general case: we will work with orders over Dedekind domains.

3. TAMENESS

The concept of tameness will play an important role in later sections. In this section we fix a field k and let A be commutative finite k -algebra. Recall that A is an artinian ring and has only finitely many maximal ideals ([1], Chapter 8). We have a natural trace map

$$\begin{aligned} \text{Tr}_{A/k} : A &\rightarrow k \\ x &\mapsto \text{Tr}(\cdot x) \end{aligned}$$

where $\cdot x : A \rightarrow A$ is the multiplication by x map and $\text{Tr}(\cdot x)$ is the standard trace of an endomorphism on a vector space over k .

Definition 3.1. Consider the symmetric k -bilinear form

$$\begin{aligned} \langle \cdot, \cdot \rangle : A \times A &\rightarrow k \\ \langle x, y \rangle &\mapsto \text{Tr}_{A/k}(xy). \end{aligned}$$

The radical of this form, A^\perp , is defined to be $\{x \in A : \text{Tr}(xA) = 0\}$. We say that A is *tame* over k if A^\perp is equal to the nilradical of A . If A is not tame, it is called *wild*.

We say that A is *finite étale* if $\langle \cdot, \cdot \rangle$ is non-degenerate, that is, if the natural map $A \rightarrow \text{Hom}(A, k)$ which maps $x \in A$ to $\langle x, \cdot \rangle$ is an isomorphism of k -modules. This is easily seen to be equivalent to saying that the discriminant $\Delta(A/k)$ of A over k is nonzero. Another equivalent notion is that A is isomorphic to a finite product of finite separable field extensions of k ([8], Theorem 2.7).

Remark 3.2. In Definition 3.1 it is always true that the nilradical is contained in the radical of $\langle \cdot, \cdot \rangle$.

Definition 3.3. A prime $\mathfrak{p} \subset A$ is called *wild* if $(A/\mathfrak{p})/k$ is inseparable or $\text{char}(k) \mid \text{length}_{A_\mathfrak{p}}(A_\mathfrak{p})$. If \mathfrak{p} is not wild, it is called *tame*.

Proposition 3.4. *The radical of the algebra A is equal to the intersection of all tame primes. The algebra A is tame if and only if all primes of A are tame. Furthermore, if A is wild, then $\dim_k(A) \geq \dim_k(A^\perp) \geq \text{char}(k) > 0$.*

For the proof, we need the following lemma.

Lemma 3.5 (Trace formula). *We have*

$$\text{Tr}_{A/k}(x) = \sum_{\mathfrak{p} \in \text{Spec}(A)} e_{\mathfrak{p}} \cdot \text{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p})$$

where $e_{\mathfrak{p}} = \text{length}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}})$.

Proof. First suppose that (A, \mathfrak{p}) is a local ring. Since A satisfies the descending and ascending chain conditions, there is a composition series $A = M_0 \supseteq M_1 \supseteq \dots \supseteq M_{e_{\mathfrak{p}}} = 0$ where the M_i are A -modules and $M_i/M_{i-1} \cong A/\mathfrak{p}$ (see [1], Proposition 6.8). As the trace is additive on exact sequences, we find

$$\text{Tr}_{A/k}(x) = \sum_{i=1}^{e_{\mathfrak{p}}} \text{Tr}_{(M_i/M_{i-1})/k}(x).$$

Since we have isomorphisms $M_i/M_{i-1} \cong A/\mathfrak{p}$, all the multiplication maps by x have the same trace. This shows that $\text{Tr}_{A/k}(x) = e_{\mathfrak{p}} \cdot \text{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p})$.

Now we will do the general case. We know that $A \cong \prod_{\mathfrak{p} \in \text{Spec}(A)} A_{\mathfrak{p}}$ (see [7], Exercise 10.9f). As $A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ by the natural map, we obtain

$$\text{Tr}_{A/k}(x) = \sum_{\mathfrak{p} \in \text{Spec}(A)} e_{\mathfrak{p}} \cdot \text{Tr}_{(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})/k}(x + \mathfrak{p}A_{\mathfrak{p}}) = \sum_{\mathfrak{p} \in \text{Spec}(A)} e_{\mathfrak{p}} \cdot \text{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p}).$$

□

Proof of Proposition 3.4. The first statement is obtained from Lemma 3.5 and Proposition 3.4 from [9]. For the second statement, use the Chinese remainder theorem to see that the nilradical, which is equal to the intersection of all prime ideals, is not equal to the intersection of a strict subset of the set of prime ideals. For the third statement, notice first of all that if $\text{char}(k) = 0$, then A is tame. Suppose that \mathfrak{p} is a wild prime, then we have $\dim_k(A^\perp) \geq \dim_k(A_{\mathfrak{p}})$. We have $\dim_k(A_{\mathfrak{p}}) = e_{\mathfrak{p}} \cdot \dim_k(A/\mathfrak{p})$. As \mathfrak{p} is wild, either $e_{\mathfrak{p}}$ is divisible by $\text{char}(k)$ or A/\mathfrak{p} is an inseparable extension, with degree is divisible by $\text{char}(k)$. □

Lemma 3.6. *Suppose that $k \subseteq k' \subseteq A$ where k' is a field. If A is tame over k , then A is tame over k' .*

Proof. An element in the trace radical with respect to k' will be in the trace radical with respect to k , hence will be nilpotent by definition of tameness. □

4. ORDERS

In this section let R be a Dedekind domain.

Theorem 4.1. *Let M be a finitely generated R -module. Then the following statements are equivalent:*

- i. M is torsion-free;
- ii. M is flat;
- iii. M is projective.

Proof. i \iff ii: See [1], Exercise 9.5.

i \iff iii: See [10], Theorem 7.2. \square

Definition 4.2. Let T be a ring. Let $S = \{x \in T \mid \text{Ann}_T(x) = 0\} \subseteq T$ be the set consisting of elements that are not a zero divisor. Then we define the *total quotient ring* of T as $Q(T) = S^{-1}T$.

Theorem 4.3. Let T be a domain and let A be an T -algebra that is torsion-free as T -module and integral over T . Then $A \otimes_T Q(T) = Q(A)$.

Proof. Assume that $A \neq 0$. Then $T = T \cdot 1 \subseteq A$ as A is torsion-free. Now let $S = T \setminus \{0\}$ be the set of nonzero divisors of T and let S' be the set of nonzero divisors of A . Then $S \subseteq S'$ as A is torsion-free. We claim that S' is the saturation of S (see [1], Exercise 7). We have to show that for any $x \in S'$, there exists $y \in A$ with $xy \in S$. Let $x \in S'$. As A is integral over R , it follows that $x^n + r_{n-1}x^{n-1} + \dots + r_0 = 0$ for some $r_i \in T$. Assume that this relation is of minimal degree. We have $r_0 \neq 0$ as x is not a zero divisor. But this means that $x(x^{n-1} + r_{n-1}x^{n-2} + \dots + r_1) = -r_0 \in T \setminus \{0\} = S$. Hence $S^{-1}A = S'^{-1}A$ and we find (using [1], Proposition 3.5)

$$A \otimes_T Q(T) = A \otimes_T S^{-1}T = S^{-1}A = S'^{-1}A = Q(A).$$

\square

Definition 4.4. Let R be a Dedekind domain. Let A be an R -algebra. Then A is called an *order* over R if A is finitely generated torsion-free as an R -module and $Q(A) = A \otimes_R Q(R)$ is a finite étale algebra over $Q(R)$.

Definition 4.5. Let R be a Dedekind domain and let A over R . Let $M \subset Q(A)$ be a finitely generated R -module. Then we define the *trace dual* of M to be the R -module

$$M^\dagger = \{x \in Q(A) : \text{Tr}_{Q(A)/Q(R)}(xM) \subseteq R\}.$$

Definition 4.6. Let A be a ring. Then we define the *integral closure* of A in $Q(A)$ as

$$\overline{A} = \{a \in Q(A) : \text{there is a monic } f \in A[x] : f(a) = 0\}.$$

Lemma 4.7. Let R be a Dedekind domain and let $A \neq 0$ be an order over R . Then the following all hold:

- i. $R \subseteq A$ is integral and \overline{A} is the integral closure of R inside $Q(A)$;
- ii. every order $B \subset Q(A)$ satisfies $\text{Tr}_{Q(A)/Q(R)}(B) \subseteq R$;
- iii. $A \subseteq \overline{A} \subseteq A^\dagger$;
- iv. A^\dagger is a finitely generated R -module and A^\dagger/A is torsion as an R -module;
- v. \overline{A} is the unique maximal element (under inclusion) of the set of orders $B \subseteq Q(A)$.

Proof. i. We have $R \subseteq A$ as $A \neq 0$ is torsion-free. As A is finitely generated over R , we can apply Proposition 5.1 from [1] to see that $R \subseteq A$ is integral. The second statement follows from [1], Corollary 5.4.

ii. After enlarging B if necessary, we may assume that $B \otimes Q(R) = Q(A)$. In this case the restriction of $\text{Tr}_{Q(A)/Q(R)}$ to B is equal to the natural trace map to R on $\text{Hom}_R(B, R) \otimes_R B \cong \text{End}_R(B)$ (see [8], 4.8).

iii, iv. First notice that we have a map $A^\dagger \rightarrow \text{Hom}_R(A, R)$, that maps x to $(y \mapsto \text{Tr}_{Q(A)/Q(R)}(xy))$, and this map is injective as $Q(A)$ is an étale $Q(R)$ -algebra. Notice

that $\text{Hom}_R(A, R)$ is a noetherian R -module, as R is noetherian and $\text{Hom}_R(A, R)$ is a finitely generated R -module. Hence A^\dagger is finitely generated over R . Let $x \in \overline{A}$. Then $A[x]$ is an order, hence

$$\text{Tr}_{Q(A)/Q(R)}(A[x]) \subseteq R$$

and $x \in A^\dagger$. As $Q(A)/A$ is torsion we obtain iii and iv.

v. As all orders are integral over R , they are contained in the integral closure of R in $Q(A)$, which is just \overline{A} . As $\overline{A} \subseteq A^\dagger$ by ii, it follows that \overline{A} is finitely generated and torsion-free. Also $Q(\overline{A}) = Q(A)$ and hence \overline{A} is an order as well. \square

Definition 4.8. Let R be a Dedekind domain and let $A \supseteq R$ be an order over R . Let $\mathfrak{p} \subset R$ be a nonzero prime. Then A is said to be *tame* at \mathfrak{p} if $A/\mathfrak{p}A$ is tame as an R/\mathfrak{p} -algebra. If A is not tame at \mathfrak{p} , it is called *wild* at \mathfrak{p} .

Example 4.9. Let $K \supset \mathbf{Q}$ be a number field. Let $p \in \mathbf{Z}$ be prime. Then according to the usual definition of tameness, p is called tame if $p \nmid e(\mathfrak{p}/p)$ for all $\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$ with $\mathfrak{p} \cap \mathbf{Z} = (p)$. Here $e(\mathfrak{p}/p)$ is defined by $p\mathcal{O}_K = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K): \mathfrak{p} \cap \mathbf{Z} = (p)} \mathfrak{p}^{e(\mathfrak{p}/p)}$. We then find by the Chinese remainder theorem

$$\mathcal{O}_K/p\mathcal{O}_K \cong \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K): \mathfrak{p} \cap \mathbf{Z} = (p)} \mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p}/p)}.$$

From this last expression we deduce that $e_{\mathfrak{p}/p\mathcal{O}_K} = e(\mathfrak{p}/p)$. As \mathbf{F}_p is a perfect field, we see that the two definitions of tameness are the same in this case.

5. ORDERS AND LOCALIZATION

In many of the coming theorems, it is useful to focus on only one prime $\mathfrak{p} \subset R$. This is why we use the notion of localization. We have the following lemma, which summarizes the situation. The proof of this lemma follows easily from the properties of localization (see [1]).

Lemma 5.1. *The following assertions all hold.*

- i. $A_{\mathfrak{p}}$ is an order over $R_{\mathfrak{p}}$;
- ii. $Q(A_{\mathfrak{p}}) = Q(A)$;
- iii. $(A^\dagger)_{\mathfrak{p}} = (A_{\mathfrak{p}})^\dagger$ and $(A^\dagger/A)_{\mathfrak{p}} \cong (A_{\mathfrak{p}})^\dagger/A_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$ -modules;
- iv. $\overline{A}_{\mathfrak{p}} = \overline{A_{\mathfrak{p}}}$ and $(\overline{A}/A)_{\mathfrak{p}} \cong \overline{A_{\mathfrak{p}}}/A_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$ -modules;
- v. A is tame at \mathfrak{p} if and only if $A_{\mathfrak{p}}$ is tame at $\mathfrak{p}R_{\mathfrak{p}}$.

Lemma 5.2. *We have $\overline{A}/A \cong \bigoplus_{\mathfrak{p} \in \text{MaxSpec}(R)} (\overline{A_{\mathfrak{p}}}/A_{\mathfrak{p}})$.*

Proof. The assumptions of Theorem 2.13 of [2] are satisfied as \overline{A}/A has finite length by Lemma 4.7 iv. Hence $\overline{A}/A \cong \bigoplus_{\mathfrak{p} \in \text{MaxSpec}(R)} (\overline{A}/A)_{\mathfrak{p}}$. Now use Lemma 5.1. \square

The strength of the previous lemma is that it suffices to find the integral closure locally, and glue those local parts together to get the global integral closure.

Assume in the rest of the article that R is local with maximal ideal \mathfrak{p} , that is, R is a discrete valuation ring with maximal ideal $\mathfrak{p} = (\pi)$, unless stated otherwise explicitly.

6. ORDERS AND COMPLETION

Some proofs become a lot clearer if our order A is also local. This is one of the reasons why we use completions. Later we will see another reason for using completions. Recall that R is assumed to be a discrete valuation ring with maximal ideal \mathfrak{p} and that A is an order over R . Let \hat{R} be the completion of R with respect to its unique maximal ideal (see [1], Chapter 10). Then \hat{R} is a complete discrete valuation ring with maximal ideal $\mathfrak{p}\hat{R}$. We have the following lemma, which shows that completion behaves nicely with respect to the integral closure, trace duals and other things. The proof is routine and left to the reader. The reader who wants to see the proofs can look at [5].

Lemma 6.1. *The following statements hold.*

- i. *The natural map $Q(R)/R \rightarrow Q(\hat{R})/\hat{R}$ is an isomorphism.*
- ii. *$A \otimes_R \hat{R}$ is an order over R ;*
- iii. *$\overline{A \otimes_R \hat{R}} = \overline{A} \otimes_R \hat{R}$;*
- iv. *$\overline{A}/A \cong \overline{A \otimes_R \hat{R}}/A \otimes_R \hat{R}$ as \hat{R} -modules by the natural map;*
- v. *$A^\dagger \otimes_R \hat{R} \cong (A \otimes_R \hat{R})^\dagger$.*
- vi. *$A^\dagger/A \cong (A \otimes_R \hat{R})^\dagger/A \otimes_R \hat{R}$ as \hat{R} -modules by the natural map;*
- vii. *We have the following commutative diagram where the vertical maps are the natural maps and the horizontal maps look like $(\overline{x}, \overline{y}) \mapsto \overline{\text{Tr}(xy)}$ for the trace map on $Q(A \otimes_R \hat{R})$ respectively $Q(A)$:*

$$\begin{array}{ccc}
 (A \otimes_R \hat{R})^\dagger / A \otimes_R \hat{R} \times (A \otimes_R \hat{R})^\dagger / A \otimes_R \hat{R} & \longrightarrow & Q(\hat{R})/\hat{R} \\
 \uparrow & & \uparrow \\
 A^\dagger/A \times A^\dagger/A & \longrightarrow & Q(R)/R.
 \end{array}$$

- viii. *The order A is tame at \mathfrak{p} if and only if $A \otimes_R \hat{R}$ is tame at $\mathfrak{p}\hat{R}$.*

The reason to use this completion is the following theorem.

Theorem 6.2. *Let A be an order over a complete discrete valuation ring R . Then the order A has only finitely many maximal ideals and the localization $A_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m} \subset R$ is a local order over R , which is complete with respect to its maximal ideal. Furthermore we have an isomorphism $A \cong \prod_{\mathfrak{m} \in \text{Maxspec}(A)} A_{\mathfrak{m}}$ as rings by the natural map.*

Proof. Corollary 7.6 from [2] tells us that there are only finitely maximal ideals and the localization $A_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m} \subset R$ is a complete local ring which is finite over R , and $A \cong \prod_{\mathfrak{m} \in \text{Maxspec}(A)} A_{\mathfrak{m}}$. As A is projective over R and direct summands of projective modules are projective, it follows that the $A_{\mathfrak{m}}$ are also projective over R . Now notice that $A \otimes_R Q(R) = \prod_{\mathfrak{m} \in \text{Maxspec}(A)} (A_{\mathfrak{m}} \otimes_R Q(R))$ and hence

$$\Delta(Q(A)/Q(R)) = \prod_{\mathfrak{m} \in \text{Maxspec}(A)} \Delta(Q(A_{\mathfrak{m}})/Q(R)).$$

As $\Delta(Q(A)/Q(R)) \neq 0$, it follows that $\Delta(Q(A_{\mathfrak{m}})/Q(R)) \neq 0$, which shows that these $A_{\mathfrak{m}}$ are orders over R . \square

Lemma 6.3. *Let $A \subseteq A'$ be an order over a complete discrete valuation ring R with the same total quotient ring. Let $\mathfrak{m} \subset A$ be maximal. Then $A'_\mathfrak{m}$ is an order over R and $A_\mathfrak{m} \subseteq A'_\mathfrak{m} \subseteq Q(A_\mathfrak{m})$. Furthermore, we have $A'_\mathfrak{m} = \prod_{\mathfrak{m}' \supseteq \mathfrak{m}A'} A'_{\mathfrak{m}'}$ and $A' = \prod_{\mathfrak{m} \in \text{Maxspec}(A)} A'_\mathfrak{m}$.*

Proof. Notice that $A'_\mathfrak{m} = A' \otimes_A A_\mathfrak{m}$ is still a finite R -algebra as $A' \otimes_R A_\mathfrak{m}$ is. One applies Corollary 7.6 from [2] to see that $A'_\mathfrak{m} = \prod_{\mathfrak{m}' \supseteq \mathfrak{m}A'} A'_{\mathfrak{m}'}$, and as the $A'_{\mathfrak{m}'}$ are orders by Theorem 6.2, it follows that $A'_\mathfrak{m}$ is an order. Now notice that $A_\mathfrak{m} \subseteq A'_\mathfrak{m} = A' \otimes_A A_\mathfrak{m} \subseteq Q(A) \otimes_A A_\mathfrak{m} = Q(R) \otimes_R A \otimes_A A_\mathfrak{m} = Q(R) \otimes A_\mathfrak{m} = Q(A_\mathfrak{m})$ as required. The last statement follows from theorem 6.2:

$$A' = \prod_{\mathfrak{m}' \in \text{Maxspec}(A')} A'_{\mathfrak{m}'} = \prod_{\mathfrak{m} \in \text{Maxspec}(A)} A'_\mathfrak{m}.$$

□

7. GOING LOCAL DIRECTLY

In this section let (R, \mathfrak{p}) be a discrete valuation ring and let A be an order over R .

Lemma 7.1. *We have $A \otimes_R \hat{R} \cong \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} \hat{A}_\mathfrak{m}$ and the $\hat{A}_\mathfrak{m}$ are local orders over \hat{R} which are complete with respect to its maximal ideal.*

Proof. As $A/\mathfrak{p}A$ is an artinian ring, we can write $\mathfrak{p}A \supseteq \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} \mathfrak{m}^s$ for some fixed s (see [1], Chapter 8). But then we have by the Chinese remainder theorem

$$\begin{aligned} A \otimes_R \hat{R} &= \varprojlim_i A/\mathfrak{p}^i A = \varprojlim_i \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} A/\mathfrak{m}^{si} = \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} \varprojlim_i A/\mathfrak{m}^i \\ &= \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} \varprojlim_i A_\mathfrak{m}/\mathfrak{m}^i A_\mathfrak{m} = \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} \hat{A}_\mathfrak{m}. \end{aligned}$$

Hence by Theorem 6.2 we see that $\hat{A}_\mathfrak{m}$ is a local order over \hat{R} which is complete with respect to its maximal ideals. □

Lemma 7.2. *Let \mathfrak{m} be a maximal ideal of A . Then $(A^\dagger/A)_\mathfrak{m} \cong \hat{A}_\mathfrak{m}^\dagger/\hat{A}_\mathfrak{m}$ as A -modules.*

Proof. As A^\dagger/A is a module of finite length over R , it is a module of finite length over A . By Theorem 2.13 from [2] we have $A^\dagger/A = \bigoplus_{\mathfrak{m} \in \text{MaxSpec}(R)} (A^\dagger/A)_\mathfrak{m}$. By Lemma 6.1 and Lemma 7.1 we have that $A^\dagger/A \cong \bigoplus_{\mathfrak{m} \in \text{MaxSpec}(R)} \hat{A}_\mathfrak{m}^\dagger/\hat{A}_\mathfrak{m}$. We have to show that both decomposition coincide. But $\hat{A}_\mathfrak{m}^\dagger/\hat{A}_\mathfrak{m}$ is a module over $A_\mathfrak{m}$ and hence the decompositions must coincide. □

8. LOCAL ORDERS

Recall that R is assumed to be local with maximal ideal \mathfrak{p} . As we have seen in the two previous sections, by completing one obtains local orders. So let A be a local order over R with maximal ideal \mathfrak{m} .

Lemma 8.1. *The ring $\mathfrak{m} : \mathfrak{m} = \{x \in Q(A) : x\mathfrak{m} \subseteq \mathfrak{m}\}$ is an order over R and $A \subseteq \mathfrak{m} : \mathfrak{m} \subseteq \overline{A}$.*

Proof. Let $x \in \mathfrak{m} : \mathfrak{m}$. Since R is noetherian, \mathfrak{m} is a finitely generated R -module. As A is torsion-free, \mathfrak{m} is a faithful R -module. Now apply Proposition 5.1 iii from [1] to see that x is integral over A . Hence $\mathfrak{m} : \mathfrak{m} \subseteq \overline{A}$. We see that $\mathfrak{m} : \mathfrak{m}$ is finitely generated as an R -module and still torsion-free, as it is contained in $Q(A)$. As $Q(\mathfrak{m} : \mathfrak{m}) = Q(A)$, it follows that $\mathfrak{m} : \mathfrak{m}$ is an order over R . \square

The following theorem gives some equivalent criteria for testing if $A = \overline{A}$.

Theorem 8.2. *The the following statements are equivalent.*

- i. $A = \overline{A}$;
- ii. $A = \mathfrak{m} : \mathfrak{m}$;
- iii. $\mathfrak{m}(A : \mathfrak{m}) = A$;
- iv. $\mathfrak{m} : \mathfrak{m} \neq A : \mathfrak{m}$;
- v. \mathfrak{m} is principal;
- vi. A is a discrete valuation ring.

Proof. We first make a few remarks. Recall that \overline{A}/A is a finitely generated torsion R -module (Lemma 4.7). Let $r \in \mathbf{Z}_{\geq 0}$ such that $\mathfrak{p}^r \overline{A} \subseteq A$. As $A/\mathfrak{p}A$ is an artinian ring, it follows that $\mathfrak{m}^n \subseteq \mathfrak{p}A$ for some $n \in \mathbf{Z}_{\geq 0}$. Hence there exists $s \in \mathbf{Z}_{\geq 1}$ such that $\mathfrak{m}^s \overline{A} \subseteq A$.

Now we will prove that $A : \mathfrak{m} \supsetneq A$. Suppose that $A : \mathfrak{m} = A$. Pick $n \in \mathbf{Z}_{\geq 1}$ minimal such that $\mathfrak{m}^n \subseteq \mathfrak{p}A$. But then $\mathfrak{m}^{n-1} \subseteq \mathfrak{p}A : \mathfrak{m} = \mathfrak{p}(A : \mathfrak{m}) = \mathfrak{p}A$ (as \mathfrak{p} is a principal ideal), a contradiction.

i \implies ii: This follows from Lemma 8.1.

ii \implies iii: We have $\mathfrak{m} \subseteq \mathfrak{m}(A : \mathfrak{m}) \subseteq A$. Suppose that $\mathfrak{m}(A : \mathfrak{m}) \neq A$, then $\mathfrak{m}(A : \mathfrak{m}) = \mathfrak{m}$. Using this and the second remark, we conclude that $\mathfrak{m} : \mathfrak{m} = A : \mathfrak{m} \supsetneq A$, a contradiction.

iii \iff iv: Notice that $\mathfrak{m} : \mathfrak{m} \subseteq A : \mathfrak{m}$. We have $\mathfrak{m}(A : \mathfrak{m}) = A$ iff $\mathfrak{m}(A : \mathfrak{m}) \neq \mathfrak{m}$ iff $A : \mathfrak{m} \supsetneq \mathfrak{m} : \mathfrak{m}$.

iii \implies v: From $(A : \mathfrak{m})\mathfrak{m} = A$ we see that we can write $1 = \sum_{i=1}^m x_i y_i$ where $x_i \in A : \mathfrak{m}$ and $y_i \in \mathfrak{m}$. Pick i such that $x_i y_i \in A^*$. We claim that $\mathfrak{m} = (y_i)$. Indeed for $x \in \mathfrak{m}$ we find

$$x = y_i \cdot \frac{xx_i}{y_i x_i} \in (y_i).$$

v \implies vi: We know that \mathfrak{m} is principal and that A is local noetherian and has dimension 1 (as it is integral over R). This makes A into a regular local ring. By Corollary 10.14 from [2] it follows that A is a domain. Now apply Proposition 9.2 from [1] to see that A is a discrete valuation ring.

vi \implies i: Again apply Proposition 9.2 from [1] to see that A is integrally closed. \square

Theorem 8.3. *Assume that A is tame at \mathfrak{p} . Then $\mathfrak{p}A^\dagger \subseteq A$ if and only if $A = \overline{A}$. If $A \subsetneq \overline{A}$, we have $(\mathfrak{m} : \mathfrak{m})/\mathfrak{m} = A/\mathfrak{m} \oplus ((\mathfrak{m} : \mathfrak{m}) \cap \mathfrak{p}A^\dagger)/\mathfrak{m}$.*

Proof. As taking traces behaves well with respect to tensoring, we obtain the following commutative diagram

$$\begin{array}{ccccc} Q(A) & \longleftarrow & A & \longrightarrow & A/\mathfrak{p}A \\ \text{Tr}_{Q(A)/Q(R)} \downarrow & & \text{Tr}_{A/R} \downarrow & & \text{Tr}_{A/\mathfrak{p}A/R/\mathfrak{p}} \downarrow \\ Q(R) & \longleftarrow & R & \longrightarrow & R/\mathfrak{p}. \end{array}$$

Consider the symmetric bilinear form on $A/\mathfrak{p}A \times A/\mathfrak{p}A \rightarrow R/\mathfrak{p}$ obtained from $\text{Tr}_{A/\mathfrak{p}A/R/\mathfrak{p}}$. By tameness the radical of this form is $\mathfrak{m}/\mathfrak{p}A$. Hence we obtain a non-degenerate form $A/\mathfrak{m} \times A/\mathfrak{m} \rightarrow R/\mathfrak{p}$. As this trace form is induced by the trace form $\text{Tr}_{Q(A)/Q(R)}$ and \mathfrak{p} is principal, we see that

$$\mathfrak{p}A^\dagger \cap A = \{\mathfrak{p}x : \text{Tr}_{Q(A)/Q(R)}(xA) \subseteq R\} \cap A = \{y \in A : \text{Tr}_{Q(A)/Q(R)}(yA) \subseteq \mathfrak{p}\} = \mathfrak{m}.$$

\implies : Suppose that A is not integrally closed and let $T = \mathfrak{m} : \mathfrak{m}$. By Theorem 8.2 we have $T \supsetneq A$ and T is an order in $Q(A)$ by Lemma 8.1. Hence T comes with a trace form, which is induced from $\text{Tr}_{Q(A)/Q(R)}$. Notice that $\mathfrak{m} \subset T$ is an ideal. Let $p : R \rightarrow R/\mathfrak{p}$ be the reduction. Then for $x \in \mathfrak{m}$ we have $p \circ \text{Tr}_{Q(A)/Q(R)}(xT) = 0$. Now let $\varphi : T/\mathfrak{m} \times T/\mathfrak{m} \rightarrow R/\mathfrak{p}$ be the map defined by $(t + \mathfrak{m}, t' + \mathfrak{m}) \mapsto p \circ \text{Tr}_{Q(A)/Q(R)}(tt')$. Let $\psi : A/\mathfrak{m} \times A/\mathfrak{m} \rightarrow R/\mathfrak{p}$ be the map defined by $(a + \mathfrak{m}, a' + \mathfrak{m}) \mapsto p \circ \text{Tr}_{Q(A)/Q(R)}(aa')$. Then we have the following commutative diagram:

$$\begin{array}{ccc} T/\mathfrak{m} \times T/\mathfrak{m} & \xrightarrow{\varphi} & R/\mathfrak{p} \\ i \times i \uparrow & & \uparrow \text{id} \\ A/\mathfrak{m} \times A/\mathfrak{m} & \xrightarrow{\psi} & R/\mathfrak{p}. \end{array}$$

We know that $A/\mathfrak{m} \subsetneq T/\mathfrak{m}$ is non-degenerate. If denote by $^\perp$ the orthogonal complement, then by Proposition 1.7 from [3] we have

$$\begin{aligned} T/\mathfrak{m} &= A/\mathfrak{m} \perp (A/\mathfrak{m})^\perp \\ &= A/\mathfrak{m} \perp (T \cap \mathfrak{p}A^\dagger)/\mathfrak{m}, \end{aligned}$$

which proves the last statement. As $T/\mathfrak{m} \supsetneq A/\mathfrak{m}$, it follows that $(T \cap \mathfrak{p}A^\dagger)/\mathfrak{m} \neq 0$. Suppose that $\mathfrak{p}A^\dagger \subseteq A$, then we have

$$(T \cap \mathfrak{p}A^\dagger)/\mathfrak{m} = (T \cap A \cap \mathfrak{p}A^\dagger)/\mathfrak{m} = (A \cap \mathfrak{p}A^\dagger)/\mathfrak{m} = \mathfrak{m}/\mathfrak{m} = 0,$$

a contradiction.

\impliedby : By Theorem 8.2 we see that A is a discrete valuation ring. First notice that $\mathfrak{p}A^\dagger \subseteq Q(A)$ is an A -module. Now suppose that $\mathfrak{p}A^\dagger \not\subseteq A$, then $A \subseteq \mathfrak{p}A^\dagger$ (here we use that A is a discrete valuation ring). Hence we have $A \subseteq \mathfrak{p}A^\dagger \cap A = \mathfrak{m}$, a contradiction. \square

Example 8.4. Let $R = \mathbf{Z}$ and let A be an order over \mathbf{Z} which is tame at the prime p . Then the statement says that A is integrally closed at p if and only if the finite group A^\dagger/A has no element of order p^2 .

We have the following corollary.

Corollary 8.5. Assume that A is tame at \mathfrak{p} . Let $B = A^\dagger/A$. Then we have

$$(\mathfrak{m} : \mathfrak{m})/A = (\mathfrak{p}B)[\mathfrak{m}].$$

If we have $A \neq \overline{A}$, then we have

$$(\mathfrak{m} : \mathfrak{m})/A = (\mathfrak{p}B)[\mathfrak{m}] = B[\mathfrak{m}],$$

where for any A -module A' we set $A'[\mathfrak{m}] = \{x \in A' : \mathfrak{m}x = 0\}$.

Proof. We will first prove the statement if $A = \overline{A}$. Then $\mathfrak{m} : \mathfrak{m} = A$ (Theorem 8.2) and $\mathfrak{p}B = 0$ (Theorem 8.3). The statement in this case now follows directly.

Now suppose that $A \neq \overline{A}$. From Theorem 8.2 it follows that $A : \mathfrak{m} = \mathfrak{m} : \mathfrak{m}$. As $\mathfrak{m} : \mathfrak{m} \subseteq \overline{A} \subseteq A^\dagger$, it follows that $(\mathfrak{m} : \mathfrak{m})/A = (A : \mathfrak{m})/A = B[\mathfrak{m}]$. Now we obviously have $(\mathfrak{p}B)[\mathfrak{m}] \subseteq B[\mathfrak{m}]$. From Theorem 8.3 it follows that $(\mathfrak{m} : \mathfrak{m})/\mathfrak{m} = A/\mathfrak{m} + ((\mathfrak{m} : \mathfrak{m}) \cap \mathfrak{p}A^\dagger)/\mathfrak{m}$. If we now take the quotient by A/\mathfrak{m} we obtain

$$(\mathfrak{m} : \mathfrak{m})/A = (A + (\mathfrak{m} : \mathfrak{m}) \cap \mathfrak{p}A^\dagger)/A.$$

This shows that $(\mathfrak{m} : \mathfrak{m})/A \subseteq (\mathfrak{p}B)[\mathfrak{m}]$ and this finishes our proof. \square

9. THE CONNECTION BETWEEN ANISOTROPY AND THE INTEGRAL CLOSURE

In this section let R be a discrete valuation ring with maximal ideal \mathfrak{p} and let A be an order over R . If I is a nonzero ideal of R , then one easily finds $I^{-1}/R \cong_R R/I$.

Lemma 9.1. *Let $I = \text{Ann}_R(A^\dagger/A)$. Then we have the following non-degenerate symmetric R/I -bilinear form:*

$$\begin{aligned} \langle \cdot, \cdot \rangle : A^\dagger/A \times A^\dagger/A &\rightarrow I^{-1}/R \\ (x + A, y + A) &\mapsto \text{Tr}_{Q(A)/Q(R)}(xy) + R. \end{aligned}$$

Proof. One easily sees that this map is well-defined. We will give a sketch of the rest of the proof, see [5] Lemma 4.1.3 for the details. As $Q(A)$ is a finite étale $Q(R)$ -algebra, it follows that the natural map $A^\dagger \rightarrow \text{Hom}_R(A, R)$ is an isomorphism. One can use this to show that $A = A^{\dagger\dagger}$. The non-degeneracy then follows from this and the fact that $\text{length}_R(A^\dagger/A) = \text{length}_R(\text{Hom}_R(A^\dagger/A, I^{-1}/R))$. \square

Lemma 9.2. *Let the notation be as in Lemma 9.1. Suppose that \overline{A} is tame at \mathfrak{p} . Then $C = \overline{A}/A \subseteq A^\dagger/A$ satisfies $\mathfrak{p}C^\perp \subseteq C \subseteq C^\perp$.*

Proof. A simple calculation shows that $C^\perp = \overline{A}^\dagger/A$. As $\overline{A} \subseteq \overline{A}^\dagger$ by Lemma 4.7 we have $C \subseteq C^\perp$. The tameness assumption on \overline{A} implies by Theorem 8.3 that $\mathfrak{p}\overline{A}^\dagger \subseteq \overline{A}$ and hence that $\mathfrak{p}(R/I)\overline{A}^\dagger/A \subseteq \overline{A}/A$ and hence $\mathfrak{p}(R/I)C^\perp \subseteq C$. \square

Notice that R/I from the previous lemma is an artinian principal ideal ring. This lemma forms the connection between the integral closure and anisotropy. We recall some definitions from [6] first. Let (R', \mathfrak{m}) be an artinian local principal ideal ring and let n be its length. Let M be a finitely generated R' -module. Let N be an R' -module such that $N \cong_{R'} R'$ and let $\langle \cdot, \cdot \rangle : M \times M \rightarrow N$ be a non-degenerate symmetric R' -bilinear form. The *radical root* of $(M, \langle \cdot, \cdot \rangle)$ is now defined as

$$\text{rr}(M) = \bigcap_{L \subseteq M : \mathfrak{m}L^\perp \subseteq L \subseteq L^\perp} L,$$

where all L are R' -modules. We define the *lower root* of M as follows:

$$\text{lr}(M) = \sum_{k=0}^n (\mathfrak{m}^k M \cap M[\mathfrak{m}^k]),$$

where $M[\mathfrak{m}^k] = \{x \in M : \mathfrak{m}^k x = 0\}$. The form $\langle \cdot, \cdot \rangle$ is called *anisotropic* if the lower root of M is the unique submodule L of M satisfying $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$. We remark that in [6] it is shown how to calculate $\text{lr}(M)$ and check if a form is anisotropic. In [6] a formula is given for $\text{rr}(M)$ if $\text{char}(R/\mathfrak{m}) \neq 2$. We have the following lemma.

Lemma 9.3. *Assume that $\langle , \rangle : M \times M \rightarrow N$ is non-degenerate. The following statements hold.*

- i. *Suppose that M is cyclic. Then \langle , \rangle is anisotropic.*
- ii. *Suppose that M is generated by two elements and $\text{length}_{R'}(M)$ is odd. Then \langle , \rangle is anisotropic.*

Proof. See [6] Remark 5.3. □

We can now give the connection between anisotropy and the integral closure.

Theorem 9.4. *Suppose that \overline{A} is tame at \mathfrak{p} . Let $B = A^\dagger/A$ and let $I = \text{Ann}_R(A^\dagger/A)$. Consider the form \langle , \rangle from Lemma 9.1. Let $D \subset A^\dagger$ be such that $D/A = \text{rr}(B)$. Let $A[D]$ be the smallest ring inside $Q(A)$ containing A and D . Then the following statements hold.*

- i. *We have $\text{rr}(B) = D/A \subseteq A[D]/A \subseteq \overline{A}/A$.*
- ii. *Suppose that \langle , \rangle is anisotropic. Then $\overline{A}/A = \text{lr}(B)$.*
- iii. *Suppose that $\text{rr}(B)$ satisfies $\mathfrak{p}(R/I) \cdot \text{rr}(B)^\perp \subseteq \text{rr}(B)$. Assume that $A[D]$ is tame at \mathfrak{p} . Then $\overline{A}/A = A[D]/A$.*

Proof. i. We have $\text{rr}(B) = D/A \subseteq \overline{A}/A$ by Lemma 9.2. As \overline{A} is a ring, it follows that $A[D] \subseteq \overline{A}$.

ii. We directly obtain the result by definition of anisotropy and Lemma 9.2.

iii. We know that $A[D]/A \subseteq \overline{A}/A$ by i. Notice that

$$\text{rr}(B) \subseteq A[D]/A \subseteq (A[D]/A)^\perp \subseteq \text{rr}(B)^\perp.$$

Hence $\mathfrak{p}(A[D]/A)^\perp \subseteq A[D]/A$. As $A[D]$ is an order which is tame at \mathfrak{p} and $(A[D]/A)^\perp = A[D]^\dagger/A$, we can apply Theorem 8.3 to see that $\overline{A}/A = A[D]/A$. □

Later, in Theorem 12.4, we will see that under certain hypotheses we have the surprising equality $A[D] = D$.

10. A SUFFICIENT CONDITION FOR TAMENESS

In this section we will prove a condition which implies tameness and is easy to check. Recall that R is a discrete valuation ring with prime $\mathfrak{p} = (\pi)$ and A is an order over R .

Theorem 10.1. *Let $B = A^\dagger/A$. Let A' be an R -order with $A \subseteq A' \subseteq \overline{A}$. Then A' is tame at \mathfrak{p} if for all maximal ideals $\mathfrak{m} \subset A$ we have $\dim_{R/\mathfrak{p}}(B_{\mathfrak{m}}/\mathfrak{p}B_{\mathfrak{m}}) < \text{char}(R/\mathfrak{p})$ or $\text{char}(R/\mathfrak{p}) = 0$. Furthermore, the dimensions of $B/\mathfrak{p}B$ and the trace radical of $A/\mathfrak{p}A$ over R/\mathfrak{p} are equal.*

Proof. After tensoring with $\hat{R}_{\mathfrak{p}}$, we may assume that R is a complete discrete valuation ring and that $A = \prod_{\mathfrak{m} \in \text{Maxspec}(A)} A_{\mathfrak{m}}$ and $A' = \prod_{\mathfrak{m} \in \text{Maxspec}(A)} A'_{\mathfrak{m}}$ (Lemma 6.3). Let $B' = A'^\dagger/A'$ and let $\mathfrak{m}' \in \text{Maxspec}(A')$ lying above $\mathfrak{m} = A \cap \mathfrak{m}'$. By Lemma 7.2 we have $B_{\mathfrak{m}} = A_{\mathfrak{m}}^\dagger/A_{\mathfrak{m}}$ and $B'_{\mathfrak{m}'} = A_{\mathfrak{m}'}^\dagger/A'_{\mathfrak{m}'} \subseteq A_{\mathfrak{m}}^\dagger/A'_{\mathfrak{m}}$ (Lemma 6.3). We have a natural injective map

$$A_{\mathfrak{m}}^\dagger/A'_{\mathfrak{m}} \rightarrow A_{\mathfrak{m}}^\dagger/A'_{\mathfrak{m}} \cong (A_{\mathfrak{m}}^\dagger/A_{\mathfrak{m}}) / (A'_{\mathfrak{m}}/A_{\mathfrak{m}}),$$

which shows that $B'_{\mathfrak{m}'}$ is a quotient of a submodule of $B_{\mathfrak{m}}$ and this shows that $\dim_{R/\mathfrak{p}}(B'_{\mathfrak{m}'}/\mathfrak{p}B'_{\mathfrak{m}'}) \leq \dim_{R/\mathfrak{p}}(B_{\mathfrak{m}}/\mathfrak{p}B_{\mathfrak{m}})$. Hence we can assume that $A = A'$.

If $\text{char}(R/\mathfrak{p}) = 0$, then $A/\mathfrak{p}A$ will be automatically tame.

Assume that $\text{char}(R/\mathfrak{p}) \neq 0$. Assume that $A/\mathfrak{p}A$ is wild. We have that

$$A/\mathfrak{p}A = \bigoplus_{\mathfrak{m} \supseteq \mathfrak{p}A} (A/\mathfrak{p}A)_{\mathfrak{m}} = \bigoplus_{\mathfrak{m} \supset \mathfrak{p}A} A_{\mathfrak{m}}/\mathfrak{p}A_{\mathfrak{m}}$$

(exactness of localization and Theorem 2.13 from [2]). It follows that there is a prime \mathfrak{m} such that $A_{\mathfrak{m}}/\mathfrak{p}A_{\mathfrak{m}}$ is wild. By Lemma 7.2 we may assume that A is local. Let $C = A/\mathfrak{p}A$, which we assume to be wild over R/\mathfrak{p} . Then it follows that $\dim_{R/\mathfrak{p}}(C^{\perp}) \geq \text{char}(R/\mathfrak{p})$ (Proposition 3.4). For $x \in A$ we have $x + \mathfrak{p}A \in C^{\perp}$ iff $\text{Tr}_{Q(A)/Q(R)}(xA) \subseteq (\pi)$ iff $\text{Tr}_{Q(A)/Q(R)}(\frac{x}{\pi}A) \subseteq A$ iff $\frac{x}{\pi} \in A^{\dagger}$ iff $x \in \pi A^{\dagger} = \mathfrak{p}A^{\dagger}$. Hence

$$C^{\perp} = (\mathfrak{p}A^{\dagger} \cap A) / \mathfrak{p}A.$$

We have

$$\begin{aligned} (\mathfrak{p}A^{\dagger} \cap A) / \mathfrak{p}A &= (\pi A^{\dagger} \cap A) / \pi A \\ &\cong (A^{\dagger} \cap \pi^{-1}A) / A \\ &= B[\mathfrak{p}]. \end{aligned}$$

Finally consider the following exact sequence:

$$0 \longrightarrow B[\mathfrak{p}] \longrightarrow B \xrightarrow{\cdot \pi} B \longrightarrow B/\mathfrak{p}B \longrightarrow 0.$$

The length as R -module is an additive function ([1], Proposition 6.9). Hence $\text{length}_R(B[\mathfrak{p}]) = \text{length}_R(B/\mathfrak{p}B)$, and both lengths are their dimensions over R/\mathfrak{p} . So if A is wild at \mathfrak{p} we have

$$\begin{aligned} \dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) &= \dim_{R/\mathfrak{p}}(B[\mathfrak{p}]) \\ &= \dim_{R/\mathfrak{p}}(C^{\perp}) \\ &\geq \text{char}(R/\mathfrak{p}), \end{aligned}$$

and this concludes the proof. \square

Remark 10.2. As $B/\mathfrak{p}B = \bigoplus_{\mathfrak{m} \supset \mathfrak{p}A} (B/\mathfrak{p}B)_{\mathfrak{m}} = \bigoplus_{\mathfrak{m} \supset \mathfrak{p}A} B_{\mathfrak{m}}/\mathfrak{p}B_{\mathfrak{m}}$, the condition in the above theorem is satisfied if $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) < \text{char}(R/\mathfrak{p})$

We can finally prove Theorem 2.1 from the introduction.

Proof of Theorem 2.1. Use Lemma 5.2 to reduce to the case where we work over the localization of \mathbf{Z} at p . Now use Theorem 8.3 in combination with Theorem 10.1. Here we remark that for $B = A^{\dagger}/A$ we have $\dim_{\mathbf{Z}/p\mathbf{Z}}(B/pB) \leq [K : \mathbf{Q}]$. \square

Theorem 10.3. Let $B = A^{\dagger}/A$ and suppose that $2 \neq \text{char}(R/\mathfrak{p})$. Suppose that one of the following conditions is satisfied:

- i. B is cyclic as an R -module;
- ii. B is generated as an R -module by two elements and $\text{length}_R(B)$ is odd.

Then $\overline{A}/A = \text{lr}(A^{\dagger}/A)$.

Proof. Theorem 10.1 shows that we are in a tame case. Now combine Lemma 9.3 and Theorem 9.4. \square

One can show that case i in the above lemma can never happen if $\text{char}(R/\mathfrak{p}) = 2$ (see [5] Lemma 5.4.2).

We can now also prove Theorem 2.2.

Proof of Theorem 2.2. Use Lemma 5.2 to reduce to the local case. Now use Theorem 10.3 to finish the proof. \square

Example 10.4. Theorem 2.2 is false if $2 \nmid \#G$. Let $A = \mathbf{Z}[\sqrt{5}]$. Then we have $A^\dagger/A \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2 \cdot 5\mathbf{Z}$, but $\overline{A} = \mathbf{Z}[\frac{1+\sqrt{5}}{2}] \supsetneq A$.

11. GALOIS ORDERS

In this section let R be a Dedekind domain (not necessarily a discrete valuation ring) and let A be an order over R . We will present another condition for tameness in the case that a group G acts in a nice way on A (as will be explained later).

Definition 11.1. Let S be a nonzero K -algebra where K is a field and let G be a group acting on A through K -automorphisms. Then S is called a *finite Galois algebra* over K if S is a finite étale K -algebra, $\#G = \dim_K(S)$ and $S^G = K$.

Remark 11.2. There are many other equivalent definitions of finite Galois algebras. One of the statements is that S is a Galois algebra with group G if and only if S is isomorphic as a K -algebra with G -action to ${}_H\text{Map}(G, L)$ where L/K is a Galois extension with group H together with an embedding $H \rightarrow G$.

Remark 11.3. Let S be a finite Galois algebra over K with group G . Let $K \rightarrow K'$ be a morphism of fields. Then $S \otimes_K K'$ is still a finite Galois algebra over K' with group G .

Definition 11.4. Let G be a finite group acting on A by R -algebra automorphisms. Then G acts naturally on $Q(A) = A \otimes_R Q(R)$ by $Q(R)$ -algebra automorphisms. We call A a *Galois order* over R with group G if $Q(A)$ together with G is a finite Galois algebra over $Q(R)$. Remark that in such a case we have $A^G = Q(A)^G \cap A = Q(R) \cap A = R$.

Example 11.5. Let K be a number field which is Galois over \mathbf{Q} with group G . Then any order A stable under G is a Galois order with group $\{g|_A : g \in G\}$.

For a prime $\mathfrak{q} \subset A$ lying over $\mathfrak{p} \subset R$

Definition 11.6. Let $\mathfrak{q} \subset A$ be a prime lying over $\mathfrak{p} \subset R$. We define the *decomposition group* of \mathfrak{q} over \mathfrak{p} to be $G_{\mathfrak{q}/\mathfrak{p}} = \{g \in G : g(\mathfrak{q}) = \mathfrak{q}\}$. Consider the natural map $\varphi : G_{\mathfrak{q}/\mathfrak{p}} \rightarrow \text{Aut}_{R/\mathfrak{p}}(A/\mathfrak{q})$. Then we define the *inertia group* of \mathfrak{q} over \mathfrak{p} to be $I_{\mathfrak{q}/\mathfrak{p}} = \ker(\varphi) \subseteq G_{\mathfrak{q}/\mathfrak{p}}$.

Lemma 11.7. Let B be a commutative ring and $G \subseteq \text{Aut}(B)$ a finite group. If $\varphi, \psi : B \rightarrow k$ are ring morphisms to a domain k that coincide on B^G , then $\varphi = \psi \circ g$ for some $g \in G$.

Proof. See [11], Lemma 15.1 for an elegant proof. \square

Lemma 11.8. Let A be a Galois order with group G over R . Let $\mathfrak{p} \subset R$ be prime and let $\mathfrak{q} \subset A$ be a prime lying above \mathfrak{p} . Then the following statements hold:

- i. The group G acts transitively on the set of primes of A lying above \mathfrak{p} .
- ii. The map $\varphi : G_{\mathfrak{q}/\mathfrak{p}} \rightarrow \text{Aut}_{R/\mathfrak{p}}(A/\mathfrak{q})$ is surjective.
- iii. The extension A/\mathfrak{q} over R/\mathfrak{p} is normal.

Proof. For the first two parts we give a sketch since this is well-known.

- i. For two primes $\mathfrak{q}_1, \mathfrak{q}_2 \subset A$ above \mathfrak{p} we consider two maps $A \rightarrow A/\mathfrak{q}_i \rightarrow \overline{Q(R/\mathfrak{p})}$ (algebraic closure of $Q(R/\mathfrak{p})$) and apply Lemma 11.7.
- ii. For the second part, we consider maps $A \rightarrow A/\mathfrak{q} \xrightarrow{f} A/\mathfrak{q}$ where $f \in \text{Aut}_{R/\mathfrak{p}}(A/\mathfrak{q})$. Apply Lemma 11.7 to see that there is an element $g \in G$ that maps to f .
- iii. Take $\bar{a} \in A/\mathfrak{q}$ where $a \in A$. Then $\prod_{g \in G} (X - \bar{g}(a)) = \overline{\prod_{g \in G} (X - g(a))} \in R/\mathfrak{p}[X]$, which follows from the fact that $A^G = R$ as A is a Galois algebra. \square

The concepts defined above behave well under localization and completion.

Lemma 11.9. *Suppose that A is a Galois order over R with group G . Let $\mathfrak{p} \subset R$ be prime and let $\mathfrak{q} \subset A$ be a prime lying over \mathfrak{p} . Then the following statements hold.*

- i. $A_{\mathfrak{p}} = A \otimes_R R_{\mathfrak{p}}$ is a Galois order over $R_{\mathfrak{p}}$ with group G .
- ii. $A \otimes_R \hat{R}_{\mathfrak{p}}$ is a Galois order over $\hat{R}_{\mathfrak{p}}$ with group G .
- iii. We have $G_{\mathfrak{q}/\mathfrak{p}} = G_{\mathfrak{q}A_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}$ and $I_{\mathfrak{q}A_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}} = I_{\mathfrak{q}/\mathfrak{p}}$.
- iv. Write $A \otimes_R \hat{R}_{\mathfrak{p}} = \prod_{\mathfrak{m} \supseteq \mathfrak{p}A} \hat{A}_{\mathfrak{m}}$. Then $G_{\mathfrak{q}/\mathfrak{p}} = G_{\mathfrak{q}\hat{A}_{\mathfrak{q}}/\mathfrak{p}\hat{R}_{\mathfrak{p}}}$ and $I_{\mathfrak{q}/\mathfrak{p}} = I_{\mathfrak{q}\hat{A}_{\mathfrak{q}}/\mathfrak{p}\hat{R}_{\mathfrak{p}}}$.
- v. $\hat{A}_{\mathfrak{q}}$ is a Galois order with group $G_{\mathfrak{q}/\mathfrak{p}}$ over $\hat{R}_{\mathfrak{p}}$.

Proof. i. This is obvious since we still have the same total quotient ring.

ii. Notice that

$$Q(A \otimes_R \hat{R}) = A \otimes_R \hat{R} \otimes_{\hat{R}} Q(\hat{R}) = A \otimes_R Q(\hat{R}) = (A \otimes_R Q(R)) \otimes_{Q(R)} Q(\hat{R}).$$

Now use the fact that Galois algebras behave well with respect to base change (Remark 11.3)

iii. One can easily check this.

iv. Use the proof of Lemma 7.1 to see that the elements of $G_{\mathfrak{q}/\mathfrak{p}}$ correspond exactly to the elements which map $\hat{A}_{\mathfrak{q}}$ to itself. We have $\hat{A}_{\mathfrak{q}}/\mathfrak{q}\hat{A}_{\mathfrak{q}} = A/\mathfrak{q}$ and the natural map $G_{\mathfrak{q}\hat{A}_{\mathfrak{q}}/\mathfrak{p}\hat{R}} \rightarrow \text{Aut}(\hat{A}_{\mathfrak{q}}/\mathfrak{q}\hat{A}_{\mathfrak{q}})$ still has kernel $I_{\mathfrak{q}/\mathfrak{p}}$.

v. First of all, we have seen that $\hat{A}_{\mathfrak{q}}$ is an order (Lemma 7.1). Using the decomposition $A \otimes_R \hat{R}_{\mathfrak{p}} = \prod_{\mathfrak{m}} \hat{A}_{\mathfrak{m}}$ and the fact that G acts transitively on the set of primes (see Lemma 11.8i), we see that $\#G_{\mathfrak{q}/\mathfrak{p}} = \dim_{Q(\hat{R}_{\mathfrak{p}})}(Q(\hat{A}_{\mathfrak{q}}))$ as required. Suppose that $a \in \hat{A}_{\mathfrak{q}}$ is fixed by all elements of $G_{\mathfrak{q}/\mathfrak{p}}$. For $\mathfrak{m} \in \text{Maxspec}(A)$ let $g_{\mathfrak{m}} \in G$ be an element such that $g_{\mathfrak{m}}$ maps $\hat{A}_{\mathfrak{q}}$ to $\hat{A}_{\mathfrak{m}}$. We pick $g_{\mathfrak{q}} = \text{id} \in G$. Then consider $(g_{\mathfrak{m}}(a))_{\mathfrak{m}} \in \prod_{\mathfrak{m}} \hat{A}_{\mathfrak{m}} = A \otimes_R \hat{R}_{\mathfrak{p}}$. We claim that this element is fixed by G . Indeed, if $g \in G$ maps \mathfrak{m} to \mathfrak{m}' , then $g_{\mathfrak{m}'}^{-1}gg_{\mathfrak{m}} \in G_{\mathfrak{q}/\mathfrak{p}}$ and hence $g_{\mathfrak{m}'}^{-1}gg_{\mathfrak{m}}(a) = a$ and $gg_{\mathfrak{m}}(a) = g_{\mathfrak{m}'}(a)$ as required. As $A \otimes_R \hat{R}_{\mathfrak{p}}$ is a Galois order over $\hat{R}_{\mathfrak{p}}$, we conclude that $a \in \hat{R}_{\mathfrak{p}}$ as required. Hence the statement follows. \square

Theorem 11.10. *Let A be a Galois order over R with group G . Let \mathfrak{q} be a prime of A and let $\mathfrak{p} = \mathfrak{q} \cap R$. Then A is tame at \mathfrak{p} if and only if $\text{char}(R/\mathfrak{p}) \nmid \#I_{\mathfrak{q}/\mathfrak{p}}$.*

Proof. As G acts transitively on the primes lying above R (Lemma 11.8), A is tame at \mathfrak{p} iff A/\mathfrak{q} is a tame R/\mathfrak{p} -algebra. By Lemma 11.8 it follows that the map $G_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}} \rightarrow \text{Aut}_{R/\mathfrak{p}}(A/\mathfrak{q})$ is surjective. This lemma also gives us that the extension A/\mathfrak{q} is normal over R/\mathfrak{p} and hence that $\#G_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}} = \#\text{Aut}_{R/\mathfrak{p}}(A/\mathfrak{q}) = [A/\mathfrak{q} : R/\mathfrak{p}]_s$, the separability degree of the extension. Let i be the inseparability

degree of this extension. Notice that we have $\dim_{Q(R)}(Q(A)) = \dim_{R/\mathfrak{p}}(A/\mathfrak{p}A)$. Indeed, both are equal to $\text{rank}_{R_{\mathfrak{p}}}(A \otimes_R R_{\mathfrak{p}})$. Then we have

$$\begin{aligned}
\#G &= \dim_{Q(R)}(Q(A)) = \dim_{R/\mathfrak{p}}(A/\mathfrak{p}A) \\
&= \sum_{\mathfrak{q}' \supset \mathfrak{p}} \dim_{R/\mathfrak{p}}((A/\mathfrak{p}A)_{\mathfrak{q}'}) \\
&= \#G/G_{\mathfrak{q}/\mathfrak{p}} \cdot \dim_{R/\mathfrak{p}}((A/\mathfrak{p}A)_{\mathfrak{q}}) \quad (\text{Lemma 11.8}) \\
&= \#G/G_{\mathfrak{q}/\mathfrak{p}} \cdot \dim_{R/\mathfrak{p}}(A/\mathfrak{q}) \cdot \text{length}_{(A/\mathfrak{p}A)_{\mathfrak{q}}}((A/\mathfrak{p}A)_{\mathfrak{q}}) \\
&= \#G/G_{\mathfrak{q}/\mathfrak{p}} \cdot i \cdot [A/\mathfrak{p} : R/\mathfrak{p}]_s \cdot e_{\mathfrak{q}/\mathfrak{p}} \\
&= \#G/G_{\mathfrak{q}/\mathfrak{p}} \cdot i \cdot \#G_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}} \cdot e_{\mathfrak{q}/\mathfrak{p}}.
\end{aligned}$$

Hence $\#I_{\mathfrak{q}/\mathfrak{p}} = i \cdot e_{\mathfrak{q}/\mathfrak{p}}$. As i is always a power of $\text{char}(R/\mathfrak{p})$, the definition of tameness of A at \mathfrak{q} is equivalent to saying that $\text{char}(R/\mathfrak{p}) \nmid i \cdot e_{\mathfrak{q}/\mathfrak{p}}$, that is, $\text{char}(R/\mathfrak{p}) \nmid \#I_{\mathfrak{q}/\mathfrak{p}}$. \square

12. QUASI-ANISOTROPY AND THE INTEGRAL CLOSURE

First we will recall the definition of quasi-anisotropy from [6]. Let M be a finitely generated module over an artinian local principal ideal ring (R', \mathfrak{p}') . Let N be an R' -module such that $N \cong_{R'} R'$ and let $\langle \cdot, \cdot \rangle : M \times M \rightarrow N$ be a non-degenerate symmetric R' -bilinear form. Then $\langle \cdot, \cdot \rangle$ is called quasi-anisotropic if for all R' -submodules $L \subseteq \text{lr}(M)$ we have $\text{lr}(L^\perp/L) = \text{lr}(M)/L$. In this case we have $\text{rr}(M) = \text{lr}(M)$ (see [6], Lemma 10.8). In [6] some other equivalent definitions of quasi-anisotropy are given which are more practical. The following lemma gives the connection between quasi-anisotropy and anisotropy (see [6], Theorem 9.4).

Lemma 12.1. *Let $\langle \cdot, \cdot \rangle : M \times M \rightarrow N$ be a non-degenerate symmetric R' -bilinear form. Then $\langle \cdot, \cdot \rangle$ is quasi-anisotropic if and only if the induced form $\langle \cdot, \cdot \rangle' : M/M[\mathfrak{p}'] \times M/M[\mathfrak{p}'] \rightarrow N/N[\mathfrak{p}']$ is anisotropic.*

We also have the following lemma (Lemma 9.5 from [6]).

Lemma 12.2. *Let $\langle \cdot, \cdot \rangle : M \times M \rightarrow N$ be a non-degenerate symmetric R' -bilinear form which is quasi-anisotropic. Let $L \subseteq \text{lr}(M)$. Then $L \subseteq L^\perp$ and the induced form $\langle \cdot, \cdot \rangle' : L^\perp/L \times L^\perp/L \rightarrow N$ is also quasi-anisotropic.*

For any ring B we define the Jacobson radical \mathfrak{r}_B to be the intersection of all maximal ideals of B .

Lemma 12.3. *Let R be a complete discrete valuation ring and let A be an order over R . Then $\mathfrak{r}_A : \mathfrak{r}_A$ is an order and A is integrally closed iff $\mathfrak{r}_A : \mathfrak{r}_A = A$.*

Proof. Write $A = \prod_{\mathfrak{m}} A_{\mathfrak{m}}$ as in Theorem 6.2, where the $A_{\mathfrak{m}}$ are local with maximal ideal $\mathfrak{m}A_{\mathfrak{m}}$. Now from Lemma 8.1 we know that $\mathfrak{r}_A : \mathfrak{r}_A = \prod_{\mathfrak{m}} (\mathfrak{m}A_{\mathfrak{m}} : \mathfrak{m}A_{\mathfrak{m}})$ is an order. We know that $\overline{A} = \prod_{\mathfrak{m}} \overline{A_{\mathfrak{m}}}$, and hence A is integrally closed iff all $A_{\mathfrak{m}}$ are integrally closed. Here one uses that total quotient ring is just the product of the total corresponding total quotient rings. By Theorem 8.2 we know that $A_{\mathfrak{m}}$ is integrally closed iff $\mathfrak{m}A_{\mathfrak{m}} : \mathfrak{m}A_{\mathfrak{m}} = A_{\mathfrak{m}}$. Hence we see that A is integrally closed iff $A = \mathfrak{r}_A : \mathfrak{r}_A$. \square

We have the following theorem. The hard part is to prove that a certain module is in fact already a ring.

Theorem 12.4. *Let A be an order over a discrete valuation ring (R, \mathfrak{p}) . Let $I \subseteq \text{Ann}_R(A^\dagger/A)$ be a nonzero ideal of R . Let $A_0 = A \otimes_R \hat{R}$ and $A_{i+1} = \mathfrak{r}_{A_i} : \mathfrak{r}_{A_i}$ for $i \geq 0$. Suppose that the A_i are tame at $\mathfrak{p}\hat{R}$. Let $B = A^\dagger/A$ and let $\langle \cdot, \cdot \rangle : B \times B \rightarrow I^{-1}/R$ be the induced form (Lemma 9.1). Suppose that $\langle \cdot, \cdot \rangle$ is quasi-anisotropic. Then $\overline{A}/A = \text{lr}(B)$.*

Proof. Assume that R is complete (Lemma 6.1). We will give a proof by induction on $s = \text{length}_R(\text{lr}(B))$. If $s = 0$ then $\mathfrak{p}B = 0$ and by Theorem 8.3 we find $\overline{A}/A = A/A = \text{lr}(B)$. Now continue by induction and assume that $s \geq 1$. We know that $\text{lr}(B) = \text{rr}(B) \subseteq \overline{A}/A \subseteq A^\dagger/A$ (Theorem 9.4 and the quasi-anisotropy). As $s \geq 1$, this implies that $A \subsetneq \overline{A}$. Now consider the order $A' = \mathfrak{r}_A : \mathfrak{r}_A$. This order A' satisfies $A \subsetneq A' \subseteq \overline{A} \subseteq A^\dagger$ (Lemma 12.3). By using Corollary 8.5 and Theorem 6.2 we have $A'/A \subseteq \mathfrak{p}B \cap B[\mathfrak{p}] \subseteq \text{lr}(B)$ (by definition of the lower root). Now use Lemma 12.2 to see that $(A'^\dagger/A)/(A'/A) \cong A'^\dagger/A'$ is still quasi-anisotropic. We have by the definition of quasi-anisotropy that $\text{lr}((A'^\dagger/A)/(A'/A)) = \text{lr}(B)/(A'/A)$, which has smaller length than $\text{lr}(B)$ (as $A \subsetneq A'$). By our induction hypothesis we have

$$\begin{aligned} \text{lr}(B)/(A'/A) &= \text{lr}((A'^\dagger/A)/(A'/A)) \cong \text{lr}(A'^\dagger/A') \\ &= \overline{A'}/A' = \overline{A}/A' \cong (\overline{A}/A)/(A'/A). \end{aligned}$$

As our maps are natural, this gives $\text{lr}(B) = \overline{A}/A$ and hence we are done.

In the proof we used tameness for \overline{A} (which is one of the A_i) and the A_i . \square

We now want some condition guaranteeing this tameness.

Lemma 12.5. *Let A be an order over a discrete valuation ring (R, \mathfrak{p}) . Let $B = A^\dagger/A$. Let $A_0 = A \otimes_R \hat{R}$ and $A_{i+1} = \mathfrak{r}_{A_i} : \mathfrak{r}_{A_i}$ for $i \geq 0$. Then the orders A_i are tame at $\mathfrak{p}\hat{R}$ if one of the following conditions is satisfied.*

- i. *For every $\mathfrak{m} \subset A$ maximal we have $\dim_{R/\mathfrak{p}}(B_{\mathfrak{m}}/\mathfrak{p}B_{\mathfrak{m}}) < \text{char}(R/\mathfrak{p})$;*
- ii. *We have $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) < \text{char}(R/\mathfrak{p})$;*
- iii. *A is a Galois order over R with group G and for some prime $\mathfrak{m} \subset A$ we have $\text{char}(R/\mathfrak{p}) \nmid \#I_{\mathfrak{m}/\mathfrak{p}}$;*
- iv. *A is a Galois order over R with group G and $\text{char}(R/\mathfrak{p}) \nmid \#G$.*

Proof. i. We know that $B_{\mathfrak{m}} = \hat{A}_{\mathfrak{m}}^\dagger/\hat{A}_{\mathfrak{m}}$ by Lemma 7.2. We have $A \otimes_R \hat{R} = \prod_{\mathfrak{m}} \hat{A}_{\mathfrak{m}}$ (Lemma 7.1). By Theorem 10.1 we know that all orders between $\hat{A}_{\mathfrak{m}}$ and $\hat{A}_{\mathfrak{m}}^\dagger$ are tame at $\mathfrak{p}\hat{R}$. Hence all orders between $A \otimes_R \hat{R}$ and $\overline{A} \otimes_R \hat{R}$ are tame (Lemma 6.3).

ii. This condition implies the first condition.

iii. If the assumption holds for a single \mathfrak{m} , it holds for all primes above \mathfrak{p} , since the inertia groups are conjugate.

By Lemma 11.9 we know that $A \otimes_R \hat{R}$ is a Galois order over \hat{R} with group G , and its inertia groups are the $I_{\mathfrak{m}/\mathfrak{p}}$ where \mathfrak{m} ranges over the primes of A lying above \mathfrak{p} . We now claim that the A_i are Galois orders with group G over \hat{R} . Indeed, as they have the same quotient field as A_0 , we just need to check that G acts on them. By induction, it is enough to check it for A_1 . First notice that \mathfrak{r}_{A_0} is stable under G . Let $x \in A_1$ and $g \in G$. Then we have

$$g(x)\mathfrak{r}_{A_0} = g(x\mathfrak{r}_{A_0}) \subseteq g(\mathfrak{r}_{A_0}) = \mathfrak{r}_{A_0}.$$

So $g(x) \in A_1$ and we are done.

We can write $A \otimes_R \hat{R} = \prod_{\mathfrak{m}} \hat{A}_{\mathfrak{m}}$ and the elements of G fixing the prime corresponding to $\hat{A}_{\mathfrak{m}}$ are exactly those who fix $\hat{A}_{\mathfrak{m}}$. But then it follows that the inertia groups of the A_i are subgroups of the $I_{\mathfrak{m}/\mathfrak{p}}$. Hence $\text{char}(R/\mathfrak{p})$ doesn't divide the order of any inertia group occurring. By Theorem 11.10 we see that all A_i are tame at $\mathfrak{p}\hat{R}$ as required.

iv. As $I_{\mathfrak{m}/\mathfrak{p}} \subseteq G_{\mathfrak{q}/\mathfrak{p}} \subseteq G$ as subgroups, we have $\#I_{\mathfrak{m}/\mathfrak{p}} \mid \#G$ and the result follows from iii. \square

13. EXAMPLES

Example 13.1. Let $f = x^4 - 20x^3 - 20x^2 + 17x + 2 \in \mathbf{Z}[x]$ and let $A = \mathbf{Z}[x]/(f(x))$. Then for the discriminant we have $\Delta(f) = 7^4 \cdot 13 \cdot 11897$ and $A^\dagger/A \cong \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/(7^3 \cdot 13 \cdot 11897)\mathbf{Z}$. There is only one prime p which might satisfy $p \mid [\bar{A} : A]$, namely 7. By Theorem 8.3 we have that $7 \mid [\bar{A} : A]$. By Lemma 12.1 and Lemma 9.3 we see that the form corresponding to the prime 7 is quasi-anisotropic. By Theorem 12.4 we have

$$\bar{A}/A = \text{lr}(A^\dagger/A) = \left(A + \frac{3\alpha^3 + \alpha^2 + 2}{7}\mathbf{Z} \right) / A.$$

Example 13.2. Let $f = x^4 - 625x^3 - 125x^2 - 15625x - 15625 \in \mathbf{Z}[x]$ and let $A = \mathbf{Z}[x]/(f(x))$. Then $\Delta(f) = 5^{20} \cdot 13 \cdot 457 \cdot 8111$. In this case $A^\dagger/A \cong \mathbf{Z}/5^3\mathbf{Z} \times \mathbf{Z}/5^7\mathbf{Z} \times \mathbf{Z}/5^{10} \cdot 13 \cdot 457 \cdot 8111\mathbf{Z}$. A calculation, which uses the algorithmic description of anisotropy from [6], shows that the form at the prime 5 is anisotropic. Now use Theorem 9.4 to get

$$\bar{A} = \text{lr}(A^\dagger/A) = \mathbf{Z} + \left(\frac{3}{3125}\alpha^3 + \frac{1}{25}\alpha \right) \mathbf{Z} + \frac{1}{125}\alpha^2\mathbf{Z} + \frac{1}{625}\alpha^3\mathbf{Z}.$$

Remark 13.3. The examples above come from algebraic number theory. One can also make examples using for example function fields.

14. A BETTER BASE RING

In many cases we can't use Theorem 10.1 and in many other situations we have the problem that vector spaces of high dimensions with an inner product are often isotropic. In practice the modules will have a large length as an R -module and this is caused by the fact that A^\dagger/A is an A -module, not only an R -module.

In this section let (R, \mathfrak{p}) be a complete discrete valuation ring and let (A, \mathfrak{m}) be a local order over R . We will find a nice ring between R and A that can be used instead of R .

Lemma 14.1. *There is a unique R -subalgebra of A , say T , such that the map $\varphi : T \rightarrow A/\mathfrak{m}$ has kernel $\mathfrak{p}T$ and image $(A/\mathfrak{m})_s$, the separable closure of R/\mathfrak{p} inside A/\mathfrak{m} . This ring T has the following additional properties:*

- i. T is free over R of rank equal to $[A/\mathfrak{m} : R/\mathfrak{p}]_s$, the separability degree of A/\mathfrak{m} over R/\mathfrak{p} ;
- ii. T is a complete discrete valuation ring with maximal ideal $\mathfrak{p}T$;
- iii. $Q(T)$ is finite étale over $Q(R)$;
- iv. A is an order over T .

Proof. We will first construct T . It follows from Theorem 6.2 that A is complete with respect to \mathfrak{m} .

Now pick $\alpha \in A$ such that $(A/\mathfrak{m})_s = (R/\mathfrak{p})[\overline{\alpha}]$. Let $f \in R[x]$ be monic of degree $[A/\mathfrak{m} : R/\mathfrak{p}]_s$ with $\overline{f}(\overline{\alpha}) = 0$. By construction we have $f(\alpha) \in \mathfrak{m}$ and $f'(\alpha) \in A^*$ (by the separability). As A is complete with respect to \mathfrak{m} , we can apply Hensel's Lemma ([2], Theorem 7.3) to find a unique $\beta \in \alpha + \mathfrak{m}$ such that $f(\beta) = 0$. Now let $T = R[\beta]$. By construction the image under φ is $(A/\mathfrak{m})_s$. As $\mathfrak{m} \cap R = \mathfrak{p}$ ([1], Corollary 5.8) it follows that $\mathfrak{p}T \subset \ker(\varphi)$. Now consider the surjective map $\overline{\varphi} : T/\mathfrak{p}T \rightarrow (A/\mathfrak{m})_s$. As the dimensions satisfy $\dim_{R/\mathfrak{p}}(T/\mathfrak{p}T) \leq [A/\mathfrak{m} : R/\mathfrak{p}]_s$, the map is injective as well.

Now we will prove the four properties for any T' satisfying the definition in the lemma.

i. Notice that R is a principal ideal domain and as A is torsion free over R , A is free over R . By assumption $T'/\mathfrak{p}T' \cong (A/\mathfrak{m})_s$, and hence T' is free over R of rank $[A/\mathfrak{m} : R/\mathfrak{p}]_s$.

ii. As $T'/\mathfrak{p}T' \cong (A/\mathfrak{m})_s$, a field, it follows that $\mathfrak{p}T$ is a maximal and principal ideal. Theorem 7.2 from [2] says that T' is complete with respect to $\mathfrak{p}T'$ and hence local. As T is a regular local ring, it is a domain by Corollary 10.14 from [2]. As the maximal ideal is principal, it is a complete discrete valuation ring by [1], Proposition 9.2.

iii. and iv. We know that $Q(A)$ is finite étale over $Q(R)$. It follows that $Q(A)$ is a finite product of finite separable field extensions over $Q(R)$. By exactness of localization and Theorem 4.3 we have the inclusions

$$Q(R) = R \otimes_R Q(R) \subseteq Q(T') = T' \otimes_R Q(R) \subseteq Q(A) = A \otimes_R Q(R).$$

We see that $Q(T')$ is a separable field extension of $Q(R)$. This shows that $Q(T')$ is finite étale over $Q(R)$ and that A is an order over T' .

We will now prove that T is unique. Suppose we have another T' which satisfies the defining properties. Consider the map $\varphi' : T' \rightarrow (A/\mathfrak{m})_s$ which has kernel $\mathfrak{p}T'$. By completeness of T' at $\mathfrak{p}T'$ it follows that there is a unique $\alpha' \in \varphi'^{-1}(\overline{\alpha}) \subset \alpha + \mathfrak{m}$ satisfying $f(\alpha') = 0$. By uniqueness of α it follows that $\alpha = \alpha' \in T'$. Hence $T' \subseteq T$. Now apply Lemma 7.4 from [4] Chapter II to see that $T' = T$. \square

Let T be as in the above lemma. We will now prove some more properties. We let A_R^\dagger respectively A_T^\dagger be the trace duals with respect to R respectively T . Similarly, T_R^\dagger is the trace dual of T with respect to R .

Lemma 14.2. *The following properties hold.*

- i. We have $\Delta(T/R) \in R^*$;
- ii. $T_R^\dagger = T$;
- iii. $A_T^\dagger = A_R^\dagger$.

Proof. i. We have the following commutative diagram:

$$\begin{array}{ccc} T & \longrightarrow & T/\mathfrak{p}T \\ \text{Tr}_{T/R} \downarrow & & \downarrow \text{Tr}_{T/\mathfrak{p}T/R/\mathfrak{p}} \\ R & \longrightarrow & R/\mathfrak{p}. \end{array}$$

By definition of T the extension $T/\mathfrak{p}T \supset R/\mathfrak{p}$ is separable, hence has nonzero discriminant. Since the discriminant behaves well with respect to tensoring, this shows that $\Delta(T/R) \in R^*$.

ii. If e_1, \dots, e_n is a basis of T over R , then it follows that $(\text{Tr}_{T/R}(e_i e_j))_{ij}$ is invertible over R and it follows directly that $T_R^\dagger = T$.

iii. We find using ii for $x \in Q(A)$:

$$\begin{aligned}
 x \in A_R^\dagger &\iff \text{Tr}_{Q(A)/Q(R)}(xA) \subseteq R \\
 &\iff \text{Tr}_{Q(T)/Q(R)}(\text{Tr}_{Q(A)/Q(T)}(xA)) \subseteq R \\
 &\iff \text{Tr}_{Q(T)/Q(R)}(T \cdot \text{Tr}_{Q(A)/Q(T)}(xA)) \subseteq R \\
 &\iff \text{Tr}_{Q(A)/Q(T)}(xA) \subseteq T_R^\dagger = T \\
 &\iff x \in A_T^\dagger.
 \end{aligned}$$

□

We directly see that for a T -module M of finite length we have

$$\begin{aligned}
 \text{lr}(M) &= \sum_{i=0}^{\infty} (\mathfrak{p}^i M \cap M[\mathfrak{p}^i]) \\
 &= \sum_{i=0}^{\infty} (\mathfrak{p}^i T M \cap M[\mathfrak{p}^i T]).
 \end{aligned}$$

This means that the lower root with respect to R is the same as with respect to T for such a module.

Lemma 14.3. *Let $T_1 \subseteq T_2$ be a local rings with maximal ideal \mathfrak{m}_1 respectively \mathfrak{m}_2 such that $\mathfrak{m}_2 \cap T_1 = \mathfrak{m}_1$. Suppose that $[T_2/\mathfrak{m}_2 : T_1/\mathfrak{m}_1] < \infty$. Let M be an T_2 -module of finite length. Then M has finite length over T_1 and we have*

$$\text{length}_{T_1}(M) = [T_2/\mathfrak{m}_2 : T_1/\mathfrak{m}_1] \cdot \text{length}_{T_2}(M).$$

Proof. This follows from the fact that $\text{length}_{T_1}(T_2/\mathfrak{m}_2) = [T_2/\mathfrak{m}_2 : T_1/\mathfrak{m}_1]$. □

For a T -module M of finite length we find $\text{length}_R(M) = \text{length}_T(M) \cdot [A/\mathfrak{m} : R/\mathfrak{p}]_s$.

Then we have the following commutative diagram, where $-$ stands for the reduction module A , T or R :

$$\begin{array}{ccc}
 A^\dagger/A \times A^\dagger/A & \xrightarrow{(\overline{x}, \overline{y}) \mapsto \overline{\text{Tr}_{Q(A)/Q(T)}(xy)}} & Q(T)/T \\
 & \searrow \varphi & \downarrow \overline{t \mapsto \text{Tr}_{Q(T)/Q(R)}(t)} \\
 & & Q(R)/R
 \end{array}$$

where $\varphi(\overline{x}, \overline{y}) = \overline{\text{Tr}_{Q(A)/Q(R)}(xy)}$.

Example 14.4. Let $f(x) = x^4 + 25x^3 + 92x^2 + 89x + 34 \in \mathbf{Z}_3[x]$. Let $A = \mathbf{Z}_3[\alpha]$ where α is a zero of f . Then A is an order as f is irreducible over \mathbf{Z} and $A \cong \mathbf{Z}[x]/(f(x)) \otimes_{\mathbf{Z}} \mathbf{Z}_3$. The ring A has just one prime ideal above 3, namely $(3, \alpha^2 + 2\alpha + 2)$, with residue field \mathbf{F}_9 . As there is a unique unramified extension of \mathbf{Z}_3 of degree 2, we know that $\mathbf{Z}_3[i] \subset A$ and this is a better ring to work over. We have over \mathbf{Z}_3 that $A^\dagger/A \cong (\mathbf{Z}_3/3^2\mathbf{Z}_3)^2$ (actually, the form is anisotropic, but one needs a calculation to see this). Over $\mathbf{Z}_3[i]$ we find $A^\dagger/A \cong \mathbf{Z}_3[i]/3^2\mathbf{Z}_3[i]$ and by Lemma 9.3 and Theorem 9.4 we know that the integral closure is given by the lower root.

15. USING THE BETTER BASE RING

Let A be an order over a discrete valuation ring (R, \mathfrak{p}) . Let C be any A -module that has finite length as an R -module. Then it has finite length as A -module ([2], Theorem 2.13). By Theorem 2.13 from [2] we have $C \cong_A \bigoplus_{\mathfrak{m} \in \text{MaxSpec}(A)} C_{\mathfrak{m}}$. We will now focus on such a factor $C_{\mathfrak{m}}$ as R -module, which still has finite length over R and $A_{\mathfrak{m}}$. We have

$$C_{\mathfrak{m}} \cong_R \bigoplus_{i \geq 1} (R/\mathfrak{p}^i)^{n(i, \mathfrak{m})}.$$

We claim that $[A/\mathfrak{m} : R/\mathfrak{p}]$ divides $n(i, \mathfrak{m})$. To see this notice that

$$((\mathfrak{p}^{i-1}C_{\mathfrak{m}})[\mathfrak{p}] + \mathfrak{p}^iC_{\mathfrak{m}})/\mathfrak{p}^iC_{\mathfrak{m}} \cong_R (R/\mathfrak{p})^{n(i, \mathfrak{m})}.$$

But the left hand side is an A -module, so by Lemma 14.3 we know that $[A/\mathfrak{m} : R/\mathfrak{p}]$ divides $n(i, \mathfrak{m})$.

We can apply the above to A^\dagger/A and \overline{A}/A . We can finally prove a local version of Theorem 2.3 from the introduction.

Theorem 15.1. *Let (R, \mathfrak{p}) be a discrete valuation ring and let A be an order over R . Let \mathfrak{m} be a maximal ideal of A and let $B = (A^\dagger/A)_{\mathfrak{m}} \cong_R \bigoplus_{i \geq 1} (R/\mathfrak{p}^i)^{n(i, \mathfrak{m})}$. Suppose that the following conditions are satisfied:*

- i. $\text{char}(A/\mathfrak{m}) = 0$ or $\text{char}(A/\mathfrak{m}) > \dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i \geq 1} n(i, \mathfrak{m})$;
- ii. *There exist $i_1, i_2 \in \mathbf{Z}_{\geq 1}$ such that*
 - $i_1 \not\equiv i_2 \pmod{2}$;
 - $n(i, \mathfrak{m}) = 0$ for all $i \notin \{1, i_1, i_2\}$;
 - $n(i, \mathfrak{m}) \in \{0, [A/\mathfrak{m} : R/\mathfrak{p}]\}$ for $i \in \{i_1, i_2\}$.

Then we have $(\overline{A}/A)_{\mathfrak{m}} = \text{lr}((A^\dagger/A)_{\mathfrak{m}})$

Proof. The idea of the proof is to complete and then work over the better base ring from the previous section. Lemma 7.1 and Lemma 7.2 allow us to assume that A is a local order with maximal ideal \mathfrak{m} over a complete discrete valuation ring. In this case we can use our better base ring T as in Lemma 14.1. If all $n(i, \mathfrak{m})$ are zero, then the conclusion of the theorem is correct. Otherwise it follows from assumption i that $\text{char}(A/\mathfrak{m}) = 0$ or $\text{char}(A/\mathfrak{m}) > [A/\mathfrak{m} : R/\mathfrak{p}] = d$. Both of these assumptions imply that $A/\mathfrak{m} \supseteq R/\mathfrak{p}$ is separable. Now let A' be any T -order between A and \overline{A} . Notice that $Q(T)$ is a finite étale $Q(R)$ -algebra (Lemma 14.1), and hence it directly follows that A' is an order over R . Theorem 10.1 and condition i imply that A' is tame at \mathfrak{p} . As $R/\mathfrak{p} \subseteq T/\mathfrak{p}T \subseteq A'/\mathfrak{p}A' = A'/\mathfrak{p}TA'$, it follows by Lemma 3.6 that A' is tame at $\mathfrak{p}T$.

The result now follows directly from Theorem 12.4 if we can show that the induced form is quasi-anisotropic. We know that $((\mathfrak{p}^{i-1}TB)[\mathfrak{p}T] + \mathfrak{p}^iTB)/\mathfrak{p}^iTB \cong_R (R/\mathfrak{p})^{n(i, \mathfrak{m})}$. Using Lemma 14.3 and the separability of $A/\mathfrak{m} \supseteq R/\mathfrak{p}$ it follows that $B \cong_T (T/\mathfrak{p}T)^{n(1, \mathfrak{m})/d} \oplus (T/\mathfrak{p}^{i_1}T)^{n(i_1, \mathfrak{m})/d} \oplus (T/\mathfrak{p}^{i_2}T)^{n(i_2, \mathfrak{m})/d}$. Now use condition ii, Lemma 12.1, Lemma 9.3 to see that our form is indeed quasi-anisotropic. \square

We can now prove the last theorem of the introduction.

Proof of Theorem 2.3. Reduce to the local case by Lemma 5.2 and use Theorem 15.1. \square

16. ACKNOWLEDGEMENTS

I would like to thank Professor Hendrik Lenstra for essentially coming up with all the new theory and for helping me to write this article. Without his help this article wouldn't be possible.

REFERENCES

- [1] M. F Atiyah, I.G. MacDonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Company, 1969
- [2] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer, 1995
- [3] R. Elman, N. Karpenko, A. Merkurjev, The Algebraic and Geometric Theory of Quadratic Forms, American Mathematical Society, 2008
- [4] R. Hartshorne, Algebraic Geometry, Springer, 1977
- [5] M. Kusters, Anisotropic modules and the integral closure, Universiteit Leiden, 2010, <http://www.math.leidenuniv.nl/scripties/KustersMaster.pdf>
- [6] M. Kusters, Anisotropic modules over artinian principal ideal rings, arXiv:1109.6483v1 [math.AC]
- [7] S. Lang, Algebra, Revised third edition, Springer-Verlag, 2002
- [8] H. Lenstra, Galois theory for Schemes, 2008, <http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf>
- [9] D. Lorenzini, An Invitation to Arithmetic Geometry, American Mathematical Society, 1996
- [10] J. P. May, Notes on Dedekind Rings, <http://www.math.uchicago.edu/~may/MISC/Dedekind.pdf>
- [11] P. Stevenhagen, The Arithmetic of Number Rings, pp. 209-266 in Algorithmic Number Theory, edited by J.P. Buhler, P. Stevenhagen, Cambridge University Press, 2008